Informe de Propuesta de Diseño y Optimización de Red Corporativa

Objetivo del Ejercicio: Analizar un escenario realista, diseñar una red completa para una organización de tamaño medio y proponer soluciones de rendimiento, segmentación y seguridad basadas en estándares industriales.

---

1. Descripción General del Diseño

a. Identificación de áreas clave y distribución física:

DataPlus S.A. es una empresa de tamaño medio con 60 empleados, operando desde un edificio principal de tres pisos. Los empleados se distribuyen en tres departamentos principales: Administración, Desarrollo y Soporte Técnico. Además, la empresa cuenta con servidores locales (de archivos y web) y requiere conectividad a Internet, así como una red de invitados.

Para un diseño óptimo, se propone la siguiente distribución lógica de los departamentos en el edificio:

Piso / Área	Departamento / Función	Posibles Características y Necesidades
Piso 1	**Administración**	**Personal de contabilidad, recursos humanos y gerencia. Potencialmente, área de recepción y salas de reuniones para visitantes. Requiere acceso seguro a sistemas administrativos y financieros.**
Piso 2	**Desarrollo**	**Programadores e ingenieros de software. Necesitan alta disponibilidad para entornos de desarrollo, acceso a repositorios de código y servidores de prueba.**
Piso 3	**Soporte Técnico**	**Personal de asistencia técnica y call center. Requiere conectividad robusta para herramientas de ticketing, sistemas de gestión de clientes y comunicación VoIP/videoconferencia.**
Cuarto de Servidores	**Servidores Locales**	**Ubicación centralizada y segura para el servidor de archivos y el servidor web local. Requiere control**

		de acceso físico y ambiente controlado (temperatura, energía).
Pisos Múltiples	**Red de Invitados (Wi-Fi)**	**Conectividad inalámbrica para visitantes en áreas comunes y salas de espera de cada piso. Acceso aislado solo a Internet.**

b. Objetivos generales del diseño de la red:

El diseño de la nueva infraestructura de red para DataPlus S.A. busca alcanzar los siguientes objetivos estratégicos:

- **Rendimiento Óptimo:** Asegurar una conectividad rápida, estable y de baja latencia para los 60 empleados, facilitando el acceso eficiente a los recursos internos (servidores) y a Internet.
- **Seguridad Integral:** Implementar políticas y mecanismos estrictos para proteger los datos corporativos, los sistemas y el tráfico de red contra accesos no autorizados y amenazas cibernéticas.
- **Segmentación Lógica:** Dividir la red en segmentos aislados (VLANs) para cada departamento, servidores y red de invitados, con el fin de contener el tráfico, limitar la propagación de incidentes de seguridad y controlar el acceso entre segmentos.
- **Alta Disponibilidad:** Garantizar la continuidad operativa de los servicios críticos, minimizando los tiempos de inactividad de servidores, conectividad a Internet y recursos compartidos.
- **Escalabilidad:** Diseñar una arquitectura flexible que permita un crecimiento futuro en el número de empleados, departamentos o la adición de nuevas tecnologías y servicios, sin requerir un rediseño completo.

2. Dispositivos de Red Utilizados

Para la implementación de la red de DataPlus S.A., se utilizarán los siguientes dispositivos de red, cada uno con una función específica:

- **Router Principal:**
    - **Justificación:** Es el punto de entrada y salida principal de la red hacia Internet, gestionando el tráfico de área ancha (WAN). Además, es fundamental para el enrutamiento entre las diferentes VLANs de la red interna, permitiendo la comunicación controlada entre departamentos y segmentos de forma segura.

- **Firewall de Borde:**
    - **Justificación:** Componente crítico para la seguridad perimetral de la red. Controlará el tráfico entrante y saliente, aplicando políticas de filtrado, prevención de intrusiones (IPS) y detección de amenazas (IDS), protegiendo la red interna de ataques externos.
- **Switches Gestionables (Core y de Acceso):**
    - **Core Switch:** Un switch de alto rendimiento ubicado en el área de servidores, que actuará como el punto central de interconexión para los switches de los pisos y los servidores. Gestionará un gran volumen de tráfico y la inter-VLAN routing (si el router no lo hace).
    - **Switches de Acceso (por piso):** Switches distribuidos en cada piso para conectar directamente los dispositivos de los usuarios finales (PCs, teléfonos IP, Access Points). Son gestionables para permitir la configuración de VLANs por puerto, garantizando la segmentación departamental.
    - **Justificación:** Su capacidad de gestión es indispensable para la implementación de VLANs, QoS y otras políticas de seguridad y rendimiento.
- **Access Points (AP) Inalámbricos:**
    - **Justificación:** Proporcionarán conectividad Wi-Fi robusta y segura en todos los pisos, con soporte para múltiples SSID (uno para empleados, otro para invitados) y protocolos de seguridad avanzados (WPA3-Enterprise).
- **Servidor de Archivos Local:**
    - **Justificación:** Centraliza el almacenamiento y el acceso a los documentos y recursos compartidos de la empresa, facilitando la colaboración y la gestión de datos.
- **Servidor Web Local:**
    - **Justificación:** Alojará aplicaciones internas de la empresa, la intranet o el sitio web local, según las necesidades operativas de DataPlus S.A.
- **UPS (Sistema de Alimentación Ininterrumpida):**
    - **Justificación:** Protegerá los dispositivos críticos de la red (router, firewall, switches core, servidores) de cortes de energía y fluctuaciones eléctricas, asegurando la continuidad del servicio y previniendo la pérdida de datos.

Roles de Red por Piso y Segmentación (VLANs)

La segmentación de la red mediante VLANs es fundamental para cumplir con las estrictas políticas de seguridad y optimizar el rendimiento. Se propone la siguiente distribución lógica y asignación de VLANs e IPs: **Tabla de Segmentación de Red (VLANs y Rangos IP)**

Piso / Área	Departamento / Función	VLAN ID	Rango IP Sugerido	Justificación del Rango IP y Número de Hosts
Piso 1	Administración	VLAN 10	192.168.10.0/24	Capacidad para hasta 254 dispositivos (aprox. 20-25 usuarios con margen de crecimiento).
Piso 2	Desarrollo	VLAN 20	192.168.20.0/24	Capacidad para hasta 254 dispositivos (aprox. 20-25 usuarios y equipos de prueba).
Piso 3	Soporte Técnico	VLAN 30	192.168.30.0/24	Capacidad para hasta 254 dispositivos (aprox. 15-20 usuarios y herramientas de soporte).
Cuarto de Servidores	Servidores	VLAN 90	192.168.90.0/28	Rango limitado a 14 hosts, adecuado para un número reducido de servidores, maximizando la seguridad y el control.
N/A	Invitados Wi-Fi	VLAN 100	192.168.100.0/24	Red completamente aislada de la red corporativa, para uso exclusivo de visitantes, con amplio margen de direcciones.
N/A	Gestión de Red	VLAN 99	192.168.99.0/28	Red dedicada para la gestión remota segura de dispositivos de red (routers, switches, APs).

Justificación de la segmentación por VLANs:

La implementación de VLANs ofrece beneficios cruciales para DataPlus S.A.:

- **Seguridad Mejorada:** Aísla el tráfico entre departamentos y de los servidores, conteniendo posibles brechas de seguridad y limitando la propagación de malware. Por ejemplo, un incidente en la VLAN de Soporte Técnico no afectaría directamente a la de Administración.
- **Optimización del Tráfico:** Reduce el tamaño de los dominios de broadcast y colisión, lo que se traduce en un mejor rendimiento general de la red al disminuir el tráfico innecesario en cada segmento.
- **Flexibilidad Administrativa:** Permite la reubicación lógica de usuarios o servicios sin necesidad de reconfigurar físicamente el cableado. Un empleado puede mantener su acceso a recursos de su departamento incluso si cambia de ubicación física dentro de un mismo switch.
- **Control Granular de Acceso:** Facilita la aplicación de políticas de seguridad y reglas de firewall específicas entre segmentos, permitiendo un control preciso sobre qué VLANs pueden comunicarse entre sí y qué recursos pueden acceder.

3. Topologías Utilizadas

Para la red de DataPlus S.A., se propone una combinación estratégica de topologías de red que optimizan el rendimiento, la redundancia, la gestión y la escalabilidad:

- **Topología Jerárquica (Core-Distribution-Access):**
    - **Aplicación:** Esta topología estructurará la red general del edificio. El **Router Principal/Firewall** actuará como el punto de interconexión con el exterior. Un **Switch Core** (en el área de servidores) será el núcleo de la red interna, interconectando los **Switches de Distribución** de cada piso. Los **Switches de Acceso** en cada departamento conectarán a los usuarios finales.
    - **Justificación:** Este modelo es ideal para organizaciones medianas a grandes. Facilita la escalabilidad al poder añadir nuevos pisos o departamentos sin afectar la estructura central. Mejora la gestión y la resolución de problemas al dividir la red en capas lógicas. Además, permite implementar políticas de seguridad y QoS de manera eficiente en la capa de distribución.

- **Topología en Estrella (en las capas de Distribución y Acceso):**
    - **Aplicación:** Dentro de cada piso, los dispositivos de usuario final (PCs, Laptops, teléfonos IP, Access Points) se conectarán directamente a un **Switch de Acceso**, formando una topología en estrella. Estos switches de acceso se conectarán, a su vez, al Switch de Distribución de su respectivo piso.
    - **Justificación:** Es la topología más común y rentable a nivel de acceso. Simplifica la administración, el diagnóstico y la resolución de fallas, ya que una falla en un dispositivo final o su cableado no afecta a otros dispositivos conectados al mismo switch.
- **Topología de Malla Parcial (para Conexiones Críticas, Opcional):**
    - **Aplicación (Opcional):** Podría implementarse una malla parcial para la interconexión entre el Router Principal, el Firewall y el Switch Core. Esto implica tener más de una ruta física entre estos componentes críticos.
    - **Justificación:** Aunque añade complejidad y costo, una malla parcial entre los componentes de red más importantes (que si fallan, detienen la red completa) proporciona alta redundancia y disponibilidad. Si un enlace o un dispositivo falla, el tráfico puede redirigirse automáticamente por una ruta alternativa, minimizando el tiempo de inactividad.

4. Segmentación y Seguridad

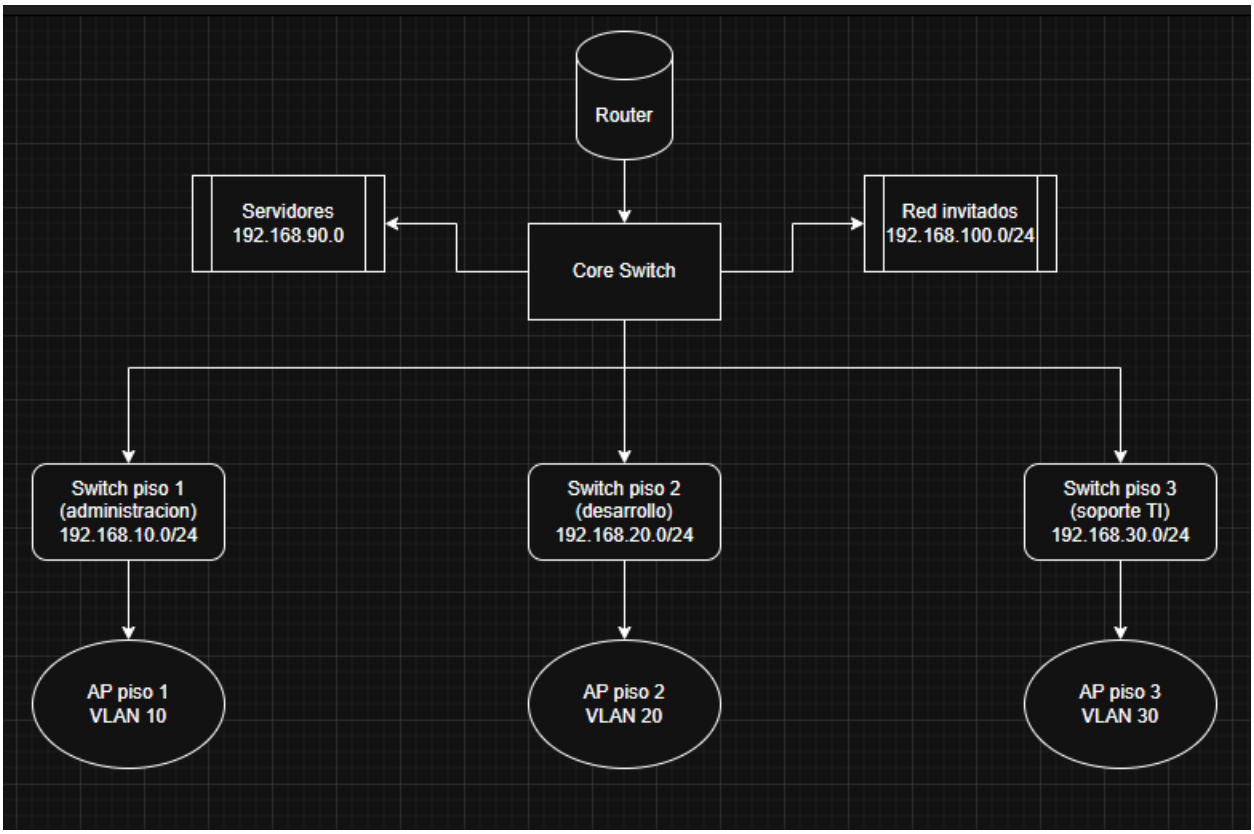
La implementación de rigurosas medidas de seguridad es un requisito fundamental para DataPlus S.A. Las VLANs propuestas en el punto 3 son la base para aplicar estas políticas:

- **Políticas de Firewall (en el Firewall de Borde y Router Principal):**
    - **Tráfico Saliente:** Permitir el acceso a Internet (puertos 80/HTTP, 443/HTTPS, 53/DNS) para las VLANs de empleados.
    - **Tráfico Entrante:** Bloquear todo el tráfico no solicitado desde Internet. Solo se abrirán puertos específicos (ej. 443/HTTPS) si el servidor web local necesita ser accesible desde el exterior, con reglas muy restrictivas.
    - **Acceso a Servidores Internos:** Se permitirán únicamente los puertos y protocolos necesarios desde las VLANs de empleados hacia la VLAN de Servidores (ej., SMB para el servidor de archivos, HTTP/HTTPS para el servidor web local).

- **Reglas de Enrutamiento InterVLAN (en el Router Principal o Switch Core Capa 3):**
    - **Comunicación entre Departamentos:** Por defecto, la comunicación directa entre VLANs de diferentes departamentos (ej., Administración a Desarrollo) estará restringida o totalmente bloqueada, salvo que exista una necesidad de negocio específica y justificada.
    - **Acceso a Servidores:** Las VLANs de Administración, Desarrollo y Soporte Técnico tendrán acceso controlado a la VLAN de Servidores, limitado a los servicios y puertos específicos que necesiten.
    - **Aislamiento de Invitados:** La VLAN de Invitados (VLAN 100) estará completamente aislada de todas las VLANs internas. Su tráfico solo podrá salir a Internet, sin posibilidad de acceder a recursos corporativos.
- **Seguridad Wi-Fi (en los Access Points):**
    - **Autenticación de Empleados:** Se configurará la red Wi-Fi para empleados con **WPA3-Enterprise** y autenticación centralizada mediante un servidor **RADIUS**, que validará las credenciales de los usuarios contra un directorio de la empresa.
    - **Red de Invitados Aislada:** Se creará una SSID separada (nombre de red Wi-Fi) para invitados, asignada a la VLAN 100, con un portal cautivo para el acceso. Esta red tendrá un ancho de banda limitado y solo permitirá la salida a Internet.
- **Medidas contra Intrusiones (IDS/IPS y Filtrado de Contenido):**
    - El Firewall de Borde incluirá funcionalidades de **Sistema de Detección y Prevención de Intrusiones (IDS/IPS)** para monitorear el tráfico en busca de, anomalías y tráfico malicioso, alertando o bloqueando las amenazas en tiempo real.
    - Se implementará **filtrado de contenido web** en el firewall o un proxy, para bloquear el acceso a sitios web maliciosos, de phishing, o a categorías de contenido no relacionadas con el trabajo.
    - **Hardening de Dispositivos:** Aplicar buenas prácticas de seguridad en la configuración de todos los dispositivos de red (cambio de contraseñas por defecto, deshabilitar servicios innecesarios, gestión remota segura con SSH/HTTPS).

5. Diagrama Lógico de Red

El siguiente diagrama representa visualmente la arquitectura de red propuesta para DataPlus S.A., mostrando la interconexión de dispositivos y la segmentación lógica mediante VLANs.



6. Escalabilidad Futura

El diseño de la red de DataPlus S.A. ha sido concebido pensando en la capacidad de crecimiento y adaptación a futuras necesidades, si la empresa duplicara su personal o agregara nuevas áreas.

- **Expansión Modular de Acceso:** La topología jerárquica permite añadir fácilmente más switches de acceso en cada piso a medida que aumente el número de empleados y dispositivos, sin afectar la infraestructura de distribución o core. Los switches actuales se seleccionarían con puertos de sobra para una expansión inicial.

- **Mejora de la Capacidad del Backbone:** Los enlaces entre la capa Core y la capa de Distribución (entre el switch principal y los switches de cada piso) pueden actualizarse progresivamente a velocidades superiores (ej., de Gigabit Ethernet a 10 Gigabit Ethernet) si el tráfico entre pisos o hacia los servidores y Internet aumenta significativamente, evitando cuellos de botella.
- **Optimización del Direccionamiento IP:** Si alguna VLAN excede su rango IP actual (/24), se podría reevaluar y ajustar el esquema de direccionamiento. Esto podría implicar expandir la subred a un prefijo más grande (ej., /23) o implementar superredes para gestionar un mayor número de hosts de forma eficiente.
- **Migración de Servicios a la Nube:** Para reducir la carga sobre la infraestructura local y aumentar la flexibilidad, se podría considerar la migración de servicios como almacenamiento de archivos, aplicaciones internas o herramientas de colaboración a plataformas en la nube (SaaS o IaaS). Esto también facilitaría el trabajo remoto y la continuidad del negocio.
- **Implementación y Refinamiento de QoS (Calidad de Servicio):** Con un mayor número de usuarios y aplicaciones, se fortalecerían las políticas de QoS para priorizar el tráfico crítico (como VoIP, videollamadas) sobre el tráfico menos sensible (como descargas), asegurando una experiencia óptima para los servicios esenciales de la empresa.
- **Aumento de Redundancia:** Si la empresa crece y la disponibilidad se vuelve aún más crítica, se podrían implementar mayores niveles de redundancia, como tener múltiples enlaces WAN (conexiones a Internet con diferentes proveedores), o configurar redundancia entre switches de distribución mediante tecnologías como Virtual Switching System (VSS) o Virtual Chassis, aumentando la resiliencia de la red.